



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,018	01/03/2001	Motoshi Ito	YAMAP0748US	3434

7590 06/22/2007  
Neil A. DuChes  
Renner, Otto, Boisselle, & Sklar, L.L.P.  
19th Floor  
1621 Euclid Avenue  
Cleveland, OH 44115

EXAMINER
----------

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

MAIL DATE	DELIVERY MODE
-----------	---------------

06/22/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Office Action Summary**

Application No.

09/754,018

Applicant(s)

ITO ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,3 and 6-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3 and 6-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 December 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

Art Unit: 2131

1 This action is in response to the communication filed on 4/12/2007.

2 **DETAILED ACTION**

3 *Continued Examination Under 37 CFR 1.114*

4 A request for continued examination under 37 CFR 1.114, including the fee set forth in  
5 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is  
6 eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)  
7 has been timely paid, the finality of the previous Office action has been withdrawn pursuant to  
8 37 CFR 1.114. Applicant's submission filed on 4/12/2007 has been entered.

9  
10 *Response to Arguments*

11 Applicant's arguments filed 4/12/2007 have been fully considered but are moot in view of  
12 the new grounds of rejection presented below.

13 The examiner further notes that the newly added limitations pertaining to the content of  
14 the recovered program is merely non-functional descriptive language, and as such does not  
15 further limit the scope of the claims, but rather provides insight into what a program could  
16 contain. There is no language that functionally links the newly added language to the system,  
17 method, or computer readable medium, and as such is merely data. However, the examiner has  
18 cited Anderson et al. as showing that programs of the nature claimed were obvious to the  
19 ordinary person skilled in the art at the time of invention.

20 All objections and rejections not presented below have been withdrawn.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirotani (US Patent Number 5,982,887), further in view of Oishi (US Patent Number 6,907,125), and further in view of Schneier (Applied Cryptography), and further in view of Elabd (US Patent Number 6,526,462), and further in view of Anderson et al. ("Navigating C++ and Object-Oriented Design"), hereinafter referred to as Anderson.

Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani also fails to disclose the use of a system on a chip design. Hirotani further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program; and a relative

Art Unit: 2131

1 address list indicating a relative address of the at least one public function in the recovered  
2 program, wherein the relative address list is provided at a prescribed location in the recovered  
3 program.

4 Oishi teaches that in order to protect against errors in a decryption system, error  
5 correction can be combined with the decryption system by encrypting error correction codes as  
6 well as the stored data and then decrypting the codes and using the codes in error correction (See  
7 Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

8 Schneier teaches that encryption and decryption can be performed in a hardware circuit  
9 (See Schneier Pages 223-225).

10 Elabd teaches that instead of using a traditional, separate component integrated circuit  
11 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

12 Anderson teaches that object-oriented designs include a public function which is to be  
13 called from outside of the recovered program and an internal function which is to be called from  
14 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
15 indicating a relative address of the at least one public function in the recovered program, wherein  
16 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
17 92-93).

18 It would have been obvious to the ordinary person skilled in the art at the time of  
19 invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by  
20 utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and  
21 further by providing a hardware decryption circuit to be used in place of the CPU decryption.  
22 This would have been obvious because the ordinary person skilled in the art would have been

Art Unit: 2131

1 motivated to protect the integrity of the program in a cost efficient manner, and further would  
2 have been motivated to increase the speed of the decryption, increase the security of the  
3 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
4 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
5 providing the components of the system on a single chip. This would have obvious because the  
6 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
7 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
8 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
9 recovered program of Hirotani by having both a public and private portion and having the public  
10 portion called from outside the program and having the private portion called from inside the  
11 public portion, and having a relative address list indicating a relative address of the at least one  
12 public function in the recovered program, wherein the relative address list is provided at a  
13 prescribed location in the program. This would have been obvious because the ordinary person  
14 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
15 from a table entry, as well as to provide encapsulation to the program.

16 Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See  
17 Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an  
18 operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including  
19 a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25  
20 Program section); a rewritable memory for storing a copy of the concealed program copied from  
21 the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the  
22 rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least

Art Unit: 2131

1 temporarily in a rewritable memory in the decryption circuit, before decryption), and a data  
2 scramble circuit for recovering the concealed program stored in the rewritable memory as a  
3 recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but  
4 failed to disclose that at least a portion of the data scramble circuit is operative to perform both a  
5 data scramble function and an error correction function. Hirotani further failed to disclose  
6 wherein a recovered program from the concealed program includes: at least a public function  
7 which is to be called from outside of the recovered program and an internal function which is to  
8 be called from inside of the recovered program; and a relative address list indicating a relative  
9 address of the at least one public function in the recovered program, wherein the relative address  
10 list is provided at a prescribed location in the recovered program.

11 Oishi teaches that in order to protect against errors in a decryption system, error  
12 correction can be combined with the decryption system by encrypting error correction codes as  
13 well as the stored data and then decrypting the codes and using the codes in error correction (See  
14 Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

15 Schneier teaches that encryption and decryption can be performed in a hardware circuit  
16 (See Schneier Pages 223-225).

17 Elabd teaches that instead of using a traditional, separate component integrated circuit  
18 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

19 Anderson teaches that object-oriented designs include a public function which is to be  
20 called from outside of the recovered program and an internal function which is to be called from  
21 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
22 indicating a relative address of the at least one public function in the recovered program, wherein

Art Unit: 2131

1 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
2 92-93).

3 It would have been obvious to the ordinary person skilled in the art at the time of  
4 invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by  
5 utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and  
6 further by providing a hardware decryption circuit to be used in place of the CPU decryption.  
7 This would have been obvious because the ordinary person skilled in the art would have been  
8 motivated to protect the integrity of the program in a cost efficient manner, and further would  
9 have been motivated to increase the speed of the decryption, increase the security of the  
10 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
11 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
12 providing the components of the system on a single chip. This would have obvious because the  
13 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
14 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
15 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
16 recovered program of Hirotani by having both a public and private portion and having the public  
17 portion called from outside the program and having the private portion called from inside the  
18 public portion, and having a relative address list indicating a relative address of the at least one  
19 public function in the recovered program, wherein the relative address list is provided at a  
20 prescribed location in the program. This would have been obvious because the ordinary person  
21 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
22 from a table entry, as well as to provide encapsulation to the program.



1           Regarding claim 6, Hirotani disclosed a method for creating a control program,  
2   comprising: a program descramble step of descrambling a portion of a control program by  
3   reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a  
4   concealed program as a portion of the control program (it was inherent in the invention of  
5   Hirotani that a portion of the control program was encrypted in order for the control program to  
6   have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control  
7   program including the concealed program in a program memory so that the control program  
8   controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines  
9   39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to  
10   perform both a data scramble function and an error correction function. Hirotani further failed to  
11   disclose wherein a recovered program from the concealed program includes: at least a public  
12   function which is to be called from outside of the recovered program and an internal function  
13   which is to be called from inside of the recovered program; and a relative address list indicating  
14   a relative address of the at least one public function in the recovered program, wherein the  
15   relative address list is provided at a prescribed location in the recovered program.

16           Oishi teaches that in order to protect against errors in a decryption system, error  
17   correction can be combined with the decryption system by encrypting error correction codes as  
18   well as the stored data and then decrypting the codes and using the codes in error correction (See  
19   Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

20           Schneier teaches that encryption and decryption can be performed in a hardware circuit  
21   (See Schneier Pages 223-225).

Art Unit: 2131

1           Elabd teaches that instead of using a traditional, separate component integrated circuit  
2 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

3           Anderson teaches that object-oriented designs include a public function which is to be  
4 called from outside of the recovered program and an internal function which is to be called from  
5 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
6 indicating a relative address of the at least one public function in the recovered program, wherein  
7 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
8 92-93).

9           It would have been obvious to the ordinary person skilled in the art at the time of  
10 invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by  
11 utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and  
12 further by providing a hardware decryption circuit to be used in place of the CPU decryption.  
13 This would have been obvious because the ordinary person skilled in the art would have been  
14 motivated to protect the integrity of the program in a cost efficient manner, and further would  
15 have been motivated to increase the speed of the decryption, increase the security of the  
16 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
17 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
18 providing the components of the system on a single chip. This would have obvious because the  
19 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
20 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
21 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
22 recovered program of Hirotani by having both a public and private portion and having the public

Art Unit: 2131

1 portion called from outside the program and having the private portion called from inside the  
2 public portion, and having a relative address list indicating a relative address of the at least one  
3 public function in the recovered program, wherein the relative address list is provided at a  
4 prescribed location in the program. This would have been obvious because the ordinary person  
5 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
6 from a table entry, as well as to provide encapsulation to the program.

7       Regarding claim 8, Hirotani disclosed a method for operating a control program,  
8 comprising: a program copying step of copying a concealed program which is a portion of the  
9 control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable  
10 memory (See rejection of claim 3 above); a program recovery step of recovering the concealed  
11 program copied by the program copying step as a recovered program by a data scramble circuit  
12 (See rejection of claim 3 above); and a program execution step of executing a non-concealed  
13 program included in the control program and the recovered program (See Hirotani Col. 6  
14 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative  
15 to perform both a data scramble function and an error correction function. Hirotani further failed  
16 to disclose wherein a recovered program from the concealed program includes: at least a public  
17 function which is to be called from outside of the recovered program and an internal function  
18 which is to be called from inside of the recovered program; and a relative address list indicating  
19 a relative address of the at least one public function in the recovered program, wherein the  
20 relative address list is provided at a prescribed location in the recovered program.

21       Oishi teaches that in order to protect against errors in a decryption system, error  
22 correction can be combined with the decryption system by encrypting error correction codes as

1 well as the stored data and then decrypting the codes and using the codes in error correction (See  
2 Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

3         Schneier teaches that encryption and decryption can be performed in a hardware circuit  
4 (See Schneier Pages 223-225).

5         Elabd teaches that instead of using a traditional, separate component integrated circuit  
6 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

7         Anderson teaches that object-oriented designs include a public function which is to be  
8 called from outside of the recovered program and an internal function which is to be called from  
9 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
10 indicating a relative address of the at least one public function in the recovered program, wherein  
11 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
12 92-93).

13         It would have been obvious to the ordinary person skilled in the art at the time of  
14 invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by  
15 utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and  
16 further by providing a hardware decryption circuit to be used in place of the CPU decryption.  
17 This would have been obvious because the ordinary person skilled in the art would have been  
18 motivated to protect the integrity of the program in a cost efficient manner, and further would  
19 have been motivated to increase the speed of the decryption, increase the security of the  
20 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
21 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
22 providing the components of the system on a single chip. This would have obvious because the

Art Unit: 2131

1 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
2 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
3 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
4 recovered program of Hirotani by having both a public and private portion and having the public  
5 portion called from outside the program and having the private portion called from inside the  
6 public portion, and having a relative address list indicating a relative address of the at least one  
7 public function in the recovered program, wherein the relative address list is provided at a  
8 prescribed location in the program. This would have been obvious because the ordinary person  
9 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
10 from a table entry, as well as to provide encapsulation to the program.

11 Regarding claim 7, the combination of Hirotani, Oishi, Schneier, Elabd, and Anderson  
12 disclosed that the program descramble step includes the steps of: creating a non-concealed  
13 program (it was inherent that the program was created at some point in order for the program to  
14 have been encrypted and downloaded); and synthesizing the concealed program and the non-  
15 concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the  
16 encrypted and non-encrypted programs are together as the program stored in program memory).

17 Regarding claim 9, the combination of Hirotani, Oishi, Schneier, Elabd, and Anderson  
18 disclosed a program erasure step of erasing the recovered program from the rewritable memory  
19 (See Hirotani Col. 6 Paragraph 6).

20  
21 Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
22 Hirotani (US Patent Number 5,982,887), further in view of Murakami et al. (US Patent Number

1 5,613,005) hereinafter referred to as Murakami, and further in view of Schneier (Applied  
2 Cryptography), and further in view of Elabd (US Patent Number 6,526,462), and further in view  
3 of Anderson et al. ("Navigating C++ and Object-Oriented Design"), hereinafter referred to as  
4 Anderson..

5 Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a  
6 microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed  
7 program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani  
8 Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only  
9 part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of  
10 the data scramble circuit is operative to perform both a data scramble function and an error  
11 correction function. Hirotani also fails to disclose the use of a system on a chip design. Hirotani  
12 further failed to disclose wherein a recovered program from the concealed program includes: at  
13 least a public function which is to be called from outside of the recovered program and an  
14 internal function which is to be called from inside of the recovered program; and a relative  
15 address list indicating a relative address of the at least one public function in the recovered  
16 program, wherein the relative address list is provided at a prescribed location in the recovered  
17 program.

18 Murakami teaches a particular encryption and decryption circuit which uses irreducible  
19 polynomials which corrects errors during decryption in order to protect against errors or missing  
20 data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

21 Schneier teaches that encryption and decryption can be performed in a hardware circuit  
22 (See Schneier Pages 223-225).

Art Unit: 2131

1           Elabd teaches that instead of using a traditional, separate component integrated circuit  
2 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

3           Anderson teaches that object-oriented designs include a public function which is to be  
4 called from outside of the recovered program and an internal function which is to be called from  
5 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
6 indicating a relative address of the at least one public function in the recovered program, wherein  
7 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
8 92-93).

9           It would have been obvious to the ordinary person skilled in the art at the time of  
10 invention to employ the teachings of Murakami and Schneier in the decryption system of  
11 Hirokuni by utilizing the decryption/error correction system of Murakami for the decryption of  
12 Hirokuni and further by providing a hardware decryption circuit to be used in place of the CPU  
13 decryption. This would have been obvious because the ordinary person skilled in the art would  
14 have been motivated to protect the integrity of the program in a cost efficient manner, and further  
15 would have been motivated to increase the speed of the decryption, increase the security of the  
16 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
17 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
18 providing the components of the system on a single chip. This would have obvious because the  
19 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
20 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
21 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
22 recovered program of Hirokuni by having both a public and private portion and having the public

Art Unit: 2131

1 portion called from outside the program and having the private portion called from inside the  
2 public portion, and having a relative address list indicating a relative address of the at least one  
3 public function in the recovered program, wherein the relative address list is provided at a  
4 prescribed location in the program. This would have been obvious because the ordinary person  
5 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
6 from a table entry, as well as to provide encapsulation to the program.

7       Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See  
8 Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an  
9 operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including  
10 a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25  
11 Program section); a rewritable memory for storing a copy of the concealed program copied from  
12 the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the  
13 rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least  
14 temporarily in a rewritable memory in the decryption circuit, before decryption), and a data  
15 scramble circuit for recovering the concealed program stored in the rewritable memory as a  
16 recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but  
17 failed to disclose that at least a portion of the data scramble circuit is operative to perform both a  
18 data scramble function and an error correction function. Hirotani further failed to disclose  
19 wherein a recovered program from the concealed program includes: at least a public function  
20 which is to be called from outside of the recovered program and an internal function which is to  
21 be called from inside of the recovered program; and a relative address list indicating a relative



Art Unit: 2131

1 address of the at least one public function in the recovered program, wherein the relative address  
2 list is provided at a prescribed location in the recovered program.

3 Murakami teaches a particular encryption and decryption circuit which uses irreducible  
4 polynomials which corrects errors during decryption in order to protect against errors or missing  
5 data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

6 Schneier teaches that encryption and decryption can be performed in a hardware circuit  
7 (See Schneier Pages 223-225).

8 Elabd teaches that instead of using a traditional, separate component integrated circuit  
9 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

10 Anderson teaches that object-oriented designs include a public function which is to be  
11 called from outside of the recovered program and an internal function which is to be called from  
12 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
13 indicating a relative address of the at least one public function in the recovered program, wherein  
14 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
15 92-93).

16 It would have been obvious to the ordinary person skilled in the art at the time of  
17 invention to employ the teachings of Murakami and Schneier in the decryption system of  
18 Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of  
19 Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU  
20 decryption. This would have been obvious because the ordinary person skilled in the art would  
21 have been motivated to protect the integrity of the program in a cost efficient manner, and further  
22 would have been motivated to increase the speed of the decryption, increase the security of the

Art Unit: 2131

1 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
2 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
3 providing the components of the system on a single chip. This would have obvious because the  
4 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
5 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
6 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
7 recovered program of Hirotani by having both a public and private portion and having the public  
8 portion called from outside the program and having the private portion called from inside the  
9 public portion, and having a relative address list indicating a relative address of the at least one  
10 public function in the recovered program, wherein the relative address list is provided at a  
11 prescribed location in the program. This would have been obvious because the ordinary person  
12 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
13 from a table entry, as well as to provide encapsulation to the program.

14       Regarding claim 6, Hirotani disclosed a method for creating a control program,  
15 comprising: a program descramble step of descrambling a portion of a control program by  
16 reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a  
17 concealed program as a portion of the control program (it was inherent in the invention of  
18 Hirotani that a portion of the control program was encrypted in order for the control program to  
19 have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control  
20 program including the concealed program in a program memory so that the control program  
21 controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines  
22 39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to

1 perform both a data scramble function and an error correction function. Hirotani further failed to  
2 disclose wherein a recovered program from the concealed program includes: at least a public  
3 function which is to be called from outside of the recovered program and an internal function  
4 which is to be called from inside of the recovered program; and a relative address list indicating  
5 a relative address of the at least one public function in the recovered program, wherein the  
6 relative address list is provided at a prescribed location in the recovered program.

7 Murakami teaches a particular encryption and decryption circuit which uses irreducible  
8 polynomials which corrects errors during decryption in order to protect against errors or missing  
9 data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

10 Schneier teaches that encryption and decryption can be performed in a hardware circuit  
11 (See Schneier Pages 223-225).

12 Elabd teaches that instead of using a traditional, separate component integrated circuit  
13 design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

14 Anderson teaches that object-oriented designs include a public function which is to be  
15 called from outside of the recovered program and an internal function which is to be called from  
16 inside of the recovered program (See Anderson Pages 175-176; and a relative address list  
17 indicating a relative address of the at least one public function in the recovered program, wherein  
18 the relative address list is provided at a prescribed location in the program (See Anderson Pages  
19 92-93).

20 It would have been obvious to the ordinary person skilled in the art at the time of  
21 invention to employ the teachings of Murakami and Schneier in the decryption system of  
22 Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of

Art Unit: 2131

1 Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU  
2 decryption. This would have been obvious because the ordinary person skilled in the art would  
3 have been motivated to protect the integrity of the program in a cost efficient manner, and further  
4 would have been motivated to increase the speed of the decryption, increase the security of the  
5 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
6 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
7 providing the components of the system on a single chip. This would have obvious because the  
8 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
9 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
10 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
11 recovered program of Hirotani by having both a public and private portion and having the public  
12 portion called from outside the program and having the private portion called from inside the  
13 public portion, and having a relative address list indicating a relative address of the at least one  
14 public function in the recovered program, wherein the relative address list is provided at a  
15 prescribed location in the program. This would have been obvious because the ordinary person  
16 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
17 from a table entry, as well as to provide encapsulation to the program.

18       Regarding claim 8, Hirotani disclosed a method for operating a control program,  
19 comprising: a program copying step of copying a concealed program which is a portion of the  
20 control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable  
21 memory (See rejection of claim 3 above); a program recovery step of recovering the concealed  
22 program copied by the program copying step as a recovered program by a data scramble circuit

(See rejection of claim 3 above); and a program execution step of executing a non-concealed program included in the control program and the recovered program (See Hirotsu Col. 6 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotsu further failed to disclose wherein a recovered program from the concealed program includes: at least a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

Anderson teaches that object-oriented designs include a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program (See Anderson Pages 175-176; and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the program (See Anderson Pages 92-93).

Art Unit: 2131

1           It would have been obvious to the ordinary person skilled in the art at the time of  
2 invention to employ the teachings of Murakami and Schneier in the decryption system of  
3 Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of  
4 Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU  
5 decryption. This would have been obvious because the ordinary person skilled in the art would  
6 have been motivated to protect the integrity of the program in a cost efficient manner, and further  
7 would have been motivated to increase the speed of the decryption, increase the security of the  
8 decryption, ease in the installation of the decryption method, and increase the efficiency of the  
9 CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by  
10 providing the components of the system on a single chip. This would have obvious because the  
11 ordinary person skilled in the art would have been motivated to produce a smaller, faster, more  
12 efficient, and less expensive product. Further still, it would have been obvious to the ordinary  
13 person skilled in the art at the time of invention to employ the teachings of Anderson in the  
14 recovered program of Hirotani by having both a public and private portion and having the public  
15 portion called from outside the program and having the private portion called from inside the  
16 public portion, and having a relative address list indicating a relative address of the at least one  
17 public function in the recovered program, wherein the relative address list is provided at a  
18 prescribed location in the program. This would have been obvious because the ordinary person  
19 skilled in the art would have been motivated to allow simple lookup schemes to call functions  
20 from a table entry, as well as to provide encapsulation to the program.

21           Regarding claim 7, the combination of Hirotani, Murakami, Schneier, Elabd, and  
22 Anderson disclosed that the program descramble step includes the steps of: creating a non-

Art Unit: 2131

1 concealed program (it was inherent that the program was created at some point in order for the  
2 program to have been encrypted and downloaded); and synthesizing the concealed program and  
3 the non-concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the  
4 encrypted and non-encrypted programs are together as the program stored in program memory).

5 Regarding claim 9, the combination of Hirotani, Murakami, Schneier, Elabd, and  
6 Anderson disclosed a program erasure step of erasing the recovered program from the rewritable  
7 memory (See Hirotani Col. 6 Paragraph 6).

### 8 9 *Conclusion*


10 Claims 1, 3, and 6-9 have been rejected.


11 Any inquiry concerning this communication or earlier communications from the  
12 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.  
13 The examiner can normally be reached on M-F 8-4.

14 If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
15 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
16 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
Matthew Henning  
Assistant Examiner  
Art Unit 2131  
6/18/2007

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100